

M

**Scalable Intrusion Detection for the Emerging Network  
"JiNao Report"**

**JiNao Report invalidates the indicated claims under 35 U.S.C. § 102(b)**

All text citations are taken from: Y. Frank Jou et al., "Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure," Technical Report CDRL A005, DARPA Order No. E296, Dept. of Computer Science North Carolina State University, April 1997, posted on the MCNC website at least as early as October 1997 [SYM\_P\_0070541-SYM\_P\_0070582], see also Jou Ex. J18 [ISS\_00357064-7105] ("JiNao Report").

Mr. Jou testified that he posted this paper on the MCNC website by April 25, 1997 and distributed an email to the DARPA intrusion detection community alerting them of the posting. Jou Tr. 73-77, 85. See also Jou Ex. J17 [SRIE 0399295].

The text included herein are merely representative samples of the disclosure in the asserted reference.

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

Claim number	Claim item	JiNao Report (patented publication)
1	A method of network surveillance, comprising:	<p>"In this project, we focus our effort on the protection of the network infrastructure since the attacks on the routers/switches have the potential of disrupting a large scale of information services on which the national defense and economy may depend. Our goal of designing this detection system is to provide a comprehensive approach which leverages on the application of novel detection techniques together with extension of some existing host-based intrusion detection methods in an internetworking environment. In particular, we will conduct logical and statistical analysis of network routing and management protocols to construct a scalable distributed intrusion detection system for the emerging internetwork environment." (1) [SYM_P_0070546]</p> <p>"Most of the current network intrusion detection efforts have taken one of the two following approaches. One approach is to collect data from separate hosts on a network for processing by a centralized intrusion detection system [2][3]. The other approach is to target network traffic at the service and protocol levels [6][7]. Our effort is close to the second approach with a few exceptions. First, we are interested in protecting network infrastructure and particularly focus on routing and management capabilities. Therefore, the target of analysis is mainly on specific protocol traffic instead of general data traffic." (2) [SYM_P_0070547]</p> <p>"The system consists of complementary functional blocks for providing comprehensive detection capabilities," (3) [SYM_P_0070548]</p> <p>See also Fig. 1. (4) [SYM_P_0070549]</p>

# Scalable Intrusion Detection for the Emerging Network “JINao Report”

358	Claim Item	JINAO Report (printed publication)
Claim number		<p>Figure 1: JINAO System Architecture.</p> <p>(4) [SYM P 0070549]</p>

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

Claim number	Claim Term	JiNao Report (printed publication)
	receiving network packets handled by a network entity;	<p>"In the early stage, intrusion detection system [sic] were designed around the analysis of a single host's audit trail. With the proliferation of computer networks, many of the intrusion detection systems began to extend the techniques to networks of computers. Most of the current network intrusion detection efforts have taken one of the two following approaches. One approach is to collect data from separate hosts on a network for processing by a centralized intrusion detection system [2][3]. The other approach is to target network traffic at the service and protocol levels [6][7]. Our effort is close to the second approach with a few exceptions. First, we are interested in protecting network infrastructure and particularly focus on routing and management capabilities. Therefore, the target of analysis is mainly on specific protocol traffic instead of general data traffic." (2). [SYM_P_0070547]</p> <p>"A local subsystem is associated with a router/switch to function as a security filter and analyze the incoming packets from its neighbors" (3) [SYM_P_0070548]</p> <p>"2.2.1.1 Interception/Redirection Module. The responsibility of the interception module is to <i>redirect</i> the target protocol information flow to the prevention layer for rule checking". (5) [SYM_P_0070550]</p> <p>"IP/IPSEC: The PDUs can be intercepted at the IP layer" (14) [SYM_P_0070559]</p> <p>See also Fig. 1 (4); [SYM_P_0070549] Fig. 3 (17) [SYM_P_0070562]</p>
	building at least one long-term and at least one short-term statistical profile from at least one measure of the network	<p>"2.2.1.3.1 Statistical Analysis Module Intrusion detection using statistical analysis is founded on the contention that behavioral signatures exist for either users' usage profiles or protocol execution patterns (in this case, network routing an management protocols) and intrusion will result in abnormal signatures. Any behavior deviating from the normal signature will be considered as an anomaly and appropriate alarms can be triggered. This module provides the capability to detect intrusions that exploit</p>

## Scalable Intrusion Detection for the Emerging Network “JiNao Report”

558 Claim number	Claim Item	JiNao Report (patented publication)
	packets	<p>previously unknown vulnerabilities.” (5) [SYM_P_0070550]</p> <p>“4.1.3.1 Statistical Analysis Module In the area of computer security, statistical analysis has been reported in various projects in the literature, for example, the NIDES project at SRI [11] Wisdom and Sense at Los Alamos National Laboratory [12], and Haystack project [13] at Haystack Laboratories. Among these examples, the NIDES project at SRI is most extensive in its scope and development. It also has the most complete documentations available to the general public. With the understanding of statistical analysis’s general applicability, we will adapt NIDES’s statistical algorithm in our approach as a starting point and modify it as necessary.</p> <p>The basic statistical approach is to compare a subject’s short-term behavior with the subject’s historical or long-term behavior. A subject is context-dependent, which can be a user of a computer system, a credit card holder, or one of the neighbor routers in the case of this project. In comparing short-term behavior with long-term behavior, the statistical component is concerned both with long-term behaviors that do not appear in short-term behavior, and with short-term behaviors that are not typical of long-term behavior.” (18) [SYM_P_0070563]</p> <p>Measures: Aspects of subject behavior are represented as measures (e.g., packet and LSA arrival frequencies in terms of their types or sources). For each measure, we will construct a probability distribution of short-term and long-term behaviors. For example, for the packet types received, the long-term probability distribution would consist of the historical probabilities with which different types of packets have been received, and the short-term probability distribution would consist of the recent probabilities with which different types [sic] packets have been received. In this case, the categories to which probabilities are attached are the names of packet types, which are learned by the system as they are received. We would classified [sic] the JiNao measures into two groups: activity intensity and audit record distribution measures. These two types of measures serve different dimensional purposes. The activity measures determine whether the volume of general activity generated in the recent past (depending on the half-life of the measure, here “recent past” corresponds to the time span of last several half-lives) is normal. These measures can detect bursts of activity or prolonged activity that is abnormal, primarily based on the volume of audit data generated. The audit record distribution measure determines whether, for recently observed activity (say, the last few</p>

## Scalable Intrusion Detection for the Emerging Network “JiNao Report”

358 Claim number	Claim/Perm	JiNaoReport (printed publication)
		<p>hundred audit records received), the types of actions being generated across neighbors are normal. For example, we might find that the last 200 routing packets received contained 120 of Hello packets, 15 of Database Description packets, 10 of Link State Request packets, 35 of Link State Update packets, and 20 of Acknowledgment [sic] packets. These data are compared to a profile of previous activity (generated over the last few months) to determine whether or not the distribution of activity types generated in the recent past (i.e., the last few hundred audit records) is unusual.</p> <p>...</p> <p>For the long-term profile, the long-term aging factor is applied to the historical data at each update, and then the new information is folded in. For the short term profile, the short-term aging factor is applied to the profile with each audit record and the current audit record is folded in.” (19) [SYM_P_0070564]</p>
the at least one measure monitoring data transfers, errors, or network connections;		<p>“A new profile (long-term and short-term) is created whenever a new subject is first encountered.” (24) [SYM_P_0070569]</p> <p>“We would classified [sic] the Ji-Nao measures into two groups: activity intensity and audit record distribution measures. These two types of measures serve different dimensional purposes. The activity measures determine whether the volume of general activity generated in the recent past (depending on the half-life of the measure, here “recent past” corresponds to the time span of last several half-lives) is normal. These measures can detect bursts of activity or prolonged activity that is abnormal, primarily based on the volume of audit data generated. The audit record distribution measure determines whether, for recently observed activity (say, the last few hundred audit records received), the types of actions being generated across neighbors are normal. For example, we might find that the last 200 routing packets received contained 120 of Hello packets, 15 of Database Description packets, 10 of Link State Request packets, 35 of Link State Update packets, and 20 of Acknowledgment [sic] packets. These data are compared to a profile of previous activity (generated over the last few months) to determine whether or not the distribution of activity types generated in the recent past (i.e., the last few hundred audit records) is unusual.” (18) [SYM_P_0070563]</p> <p>“One of the important features of the JiNao system is that it is adaptive to changing network conditions/configurations. This implies that the set of rules upon which the prevention module operates on or the threshold parameters which the statistical</p>

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

358 Claim number	Claim Term	JiNao Report (printed publication)
	comparing at least one long-term and at least one short-term statistical profile; and	<p>module uses to distinguish normal from abnormal behavior or the set of minimum detecting sequences employed by the protocol analysis module may need to be changed dynamically in response to changing network conditions. For instance, should a new point of network connectivity come up, the normal traffic profiles would need to be modified to account for the traffic from the new connection." (29) [SYM_P_0070574]</p>
	comparing at least one long-term and at least one short-term statistical profile; and	<p>See also Figure 3 ("OSPF," "SNMP," and "IP/SEC")</p> <p>"The basic statistical approach is to compare a subject's short-term behavior with the subject's historical or long-term behavior. A subject is context-dependent, which can be a user of a computer system, a credit card holder, or one of the neighbor routers in the case of this project. In comparing short-term behavior with long-term behavior, the statistical component is concerned both with long-term behaviors that do not appear in short-term behavior, and with short-term behaviors that are not typical of long-term behavior." (18) [SYM_P_0070563]</p> <p>"The Q Statistic: The degree of difference between a long-term and short-term profile for a measure is quantified using a chi-square-like statistic, comparing observation (the short-term profile) to expectation (the long-term profile)." (20) [SYM_P_0070565]</p> <p>"The range of the Q values is expressed in terms of the degree of similarity between the short-term profile and the long-term profile with larger numbers representing less similarity." (23) [SYM_P_0070568]</p> <p>"For each audit record generated by a subject, the statistical module generates a single test statistic value, denoted <math>T^2</math>, that summarizes the degree of abnormality in the subject's behavior in the near past," p. 19. [SYM_P_0070564]</p> <p>"The degree of difference between a long-term profile and short-term profile for a measure is quantified using a chi-square-like statistic, comparing observation (the short-term profile) to expectation (the long-term profile). The resultant numeral value is called Q in NIDES," (20) [SYM_P_0070565]</p>

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

Claim number	Claim term	JiNao Report (printed publication)
	determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.	<p>"Whenever short-term behavior is sufficiently unlike long-term behavior, a warning flag is raised." (18) [SYM_P_0070563]</p> <p>"The statistical component issues a warning only if the current short-term behavior is very unlike long-term behavior relative to the amount of deviation between these types of behaviors that it has seen in the past." (18) [SYM_P_0070563]</p>
2	The method of claim 1, wherein the measure monitors data transfers by monitoring network packet data transfer commands	<p>"We would classified [sic] the Ji-Nao measures into two groups: activity intensity and audit record distribution measures. These two types of measures serve different dimensional purposes. The activity measures determine whether the volume of general activity generated in the recent past (depending on the half-life of the measure, here "recent past" corresponds to the time span of last several half-lives) is normal. These measures can detect bursts of activity or prolonged activity that is abnormal, primarily based on the volume of audit data generated. The audit record distribution measure determines whether, for recently observed activity (say, the last few hundred audit records received), the types of actions being generated across neighbors are normal. For example, we might find that the last 200 routing packets received contained 120 of Hello packets, 15 of Database Description packets, 10 of Link State Request packets, 35 of Link State Update packets, and 20 of Acknowledgment [sic] packets. These data are compared to a profile of previous activity (generated over the last few months) to determine whether or not the distribution of activity types generated in the recent past (i.e., the last few hundred audit records) is unusual." (19) [SYM_P_0070564]</p>
4	The method of claim 1, wherein the measure monitors data transfers by monitoring network packet data transfer	<p>"We would classified [sic] the Ji-Nao measures into two groups: activity intensity and audit record distribution measures. These two types of measures serve different dimensional purposes. The activity measures determine whether the volume of general activity generated in the recent past (depending on the half-life of the measure, here "recent past" corresponds to the time span of last several half-lives) is normal. These measures can detect bursts of activity or prolonged activity that is abnormal, primarily</p>

## Scalable Intrusion Detection for the Emerging Network “JiNao Report”

338 Claim number	Claim Item	JiNao Report (printed publication)
	volume.	<p>based on the volume of audit data generated. The audit record distribution measure determines whether, for recently observed activity (say, the last few hundred audit records received), the types of actions being generated across neighbors are normal. For example, we might find that the last 200 routing packets received contained 120 of Hello packets, 15 of Database Description packets, 10 of Link State Request packets, 35 of Link State Update packets, and 20 of Acknowledgment [sic] packets. These data are compared to a profile of previous activity (generated over the last few months) to determine whether or not the distribution of activity types generated in the recent past (i.e., the last few hundred audit records) is unusual.” (19) [SYM_P_0070564]</p> <p>“Aspects of subject behavior are represented as measures (e.g., packet and LSA arrival frequencies in terms of their types or sources),” (19) [SYM_P_0070564]</p>
5	The method of claim 1, wherein the measure monitors network connections by monitoring network connection requests.	<p>“One of the important features of the JiNao system is that it is adaptive to changing network conditions/configurations. This implies that the set of rules upon which the prevention module operates on or the threshold parameters which the statistical module uses to distinguish normal from abnormal behavior or the set of minimum detecting sequences employed by the protocol analysis module may need to be changed dynamically in response to changing network conditions. For instance, should a new point of network connectivity come up, the normal traffic profiles would need to be modified to account for the traffic from the new connection.” (29) [SYM_P_0070574]</p> <p>See Fig. 2. (15) [SYM_P_0070560]</p> <p>See Fig. 3. (17) [SYM_P_0070562]</p> <p>“Higher-Layer Protocols: Sometimes, it is necessary to perform interception in layers beyond IP. For example, in protecting SNMP, (especially SNMPv2 and v3), the SNMP PDU might be encrypted. Under this case, we should intercept the PDU flow after the authentication and decryption process.” (14) [SYM_P_0070559]</p>

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

Claim number	Claim term	JiNao Report (printed publication)
1338		<p>"A remote management subsystem can oversee several routers/switches. Some intrusions, like doorknob rattling attack, which may be difficult to detect at a local level can be made easier by checking the global status across several routers/switches." (3) [SYM_P_0070548]</p> <p>"We would classified [sic] the Ji-Nao measures into two groups: activity intensity and audit record distribution measures. These two types of measures serve different dimensional purposes. The activity measures determine whether the volume of general activity generated in the recent past (depending on the half-life of the measure, here "recent past" corresponds to the time span of last several half-lives) is normal. These measures can detect bursts of activity or prolonged activity that is abnormal, primarily based on the volume of audit data generated. The audit record distribution measure determines whether, for recently observed activity (say, the last few hundred audit records received), the types of actions being generated across neighbors are normal. For example, we might find that the last 200 routing packets received contained 120 of Hello packets, 15 of Database Description packets, 10 of Link State Request packets, 35 of Link State Update packets, and 20 of Acknowledgment [sic] packets. These data are compared to a profile of previous activity (generated over the last few months) to determine whether or not the distribution of activity types generated in the recent past (i.e., the last few hundred audit records) is unusual." (19) [SYM_P_0070564]</p>
11	The method of claim 1, further comprising responding based on the determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.	<p>"Therefore, our design will allow for a certain degree of automated responses through the adoption of network management framework." (5) [SYM_P_0070550]</p> <p>"Ideally, as a natural extension of the current scope of the project, we expect that a remote subsystem can also implement similar detection capabilities in order to detect a larger scale of [sic] orchestrated attack. We realize that some attacks (for instance, door-knob rattling attack) can only be detected on a more global scale. One approach in dealing with these attacks is for the management applications to communicate with their local detection agents in order to form a global view of the domain surrounding this remote subsystem. The notion of global detection can be further extended to cover more than one remote</p>

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

Claim number	Claim Term	<p style="text-align: center;">JiNao Report (patented publication)</p> <p>subsystem, either in a distributed or hierarchical fashion." (6-7) [SYM_P_0070551-SYM_P_0070552]</p> <p>"Upon detection of a fault/intrusion, the LDecM must take steps to notify the appropriate network security personnel. This can be done via the use of a GUI that will make the fault/intrusion information visible on the security personnel's terminal. For less critical events, notification could be performed via email." (30) [SYM_P_0070575]</p> <p>"One of the important features of the JiNao system is that it is adaptive to changing network conditions/configurations. This implies that the set of rules upon which the prevention module operates on or the threshold parameter which the statistical module uses to distinguish normal from abnormal behavior or the set of minimum detecting sequences employed by the protocol analysis module may need to be changed dynamically in response to changing network conditions." (29) [SYM_P_0070574]</p> <p>"[B]ased on the decision it arrives at, the LDecM could initiate these changes itself. For instance, if it detected suspicious activity, it could activate additional rules in the prevention module or adjust thresholds in the statistical module. ... The LDecM interacts with the protocol engine in order to take appropriate action if an intrusion is suspected/detected. For instance, when suspicious activity is detected it may instruct the protocol engine to turn on certain special modes of operation e.g. detailed logging of messages and protocol events, log information relating to route updates and modifications etc.. The LDecM can also take appropriate defensive measures. This can include turning an interface off when a router connected via that interface has been detected to be faulty/compromised; issuing commands to undo the effects of recent route update messages, if any, from the compromised router, etc.." (30). [SYM_P_0070575]</p> <p>"Whenever short-term behavior is sufficiently unlike long-term behavior, a warning flag is raised." p. 18. [SYM_P_0070563]</p> <p>"Depending on the degree of deviation or the nature of fault/attack, an alert or alarm signal will be issued to acquire the security officer's attention." (3) [SYM_P_0070548]</p>
-----------------	------------	--

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

338 Claim number	Claim Item	JiNao Report (printed publication)
12.	The method of claim 11, wherein responding comprises transmitting an event record to a network monitor.	<p>"The notion of global detection can be further extended to cover more than one remote subsystem, either in a distributed or hierarchical fashion." (7) [SYM_P_0070552]</p> <p>"A remote management subsystem can oversee several routers/switches. Some intrusions, like doorknob rattling attack, which may be difficult to detect at a local level can be made easier by checking the global status across several routers/switches. While it is not within the scope of this project, we expect that the detection/analysis functions implemented in the local subsystem can be extended to a global level and correlate intrusion events among several routers. The management capability, which is based on SNMP framework, can logically be further extended among management nodes in a hierarchical fashion to establish a status map for an autonomous system," (3) [SYM_P_0070548]</p> <p>"2.2.1.5 Information Abstraction Module (IAM). IAM serves as an interface module between the JiNao local intrusion detection subsystem and the remote JiNao modules as well other network management applications. In propagating local intrusion detection results to the outside, the IAM aggregates local detection results and converts them into MIB format" (6) [SYM_P_0070551]</p> <p>See also figure 3 (17) [SYM_P_0070562]</p>
13	The method of claim 12, wherein transmitting the event record to a network monitor comprises transmitting the event record to a hierarchically higher network monitor.	<p>See '338 claim 12</p> <p>"A remote management subsystem can oversee several routers/switches. Some intrusions, like doorknob rattling attack, which may be difficult to detect at a local level can be made easier by checking the global status across several routers/switches. While it is not within the scope of this project, we expect that the detection/analysis functions implemented in the local subsystem can be extended to a global level and correlate intrusion events among several routers. The management capability, which is based on SNMP framework, can logically be further extended among management nodes in a hierarchical fashion to establish a status map for an autonomous system." (3) [SYM_P_0070548]</p>

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

338 Claim number	Claim Term	JiNao Report (omitted publication)
		<p>"The notion of global detection can be further extended to cover more than one remote subsystem, either in a distributed or hierarchical fashion." (7) [SYM_P_0070552]</p> <p>"We expect the detection/analysis functions implemented in the local subsystem can be extended to a global level and correlate intrusion events among several routers. The extension to a global level can be hierarchical where several regional management stations can aggregate their detection information to a higher level for establishing a global view of the routing domain status." (13) [SYM_P_0070538]</p> <p>"The following example is used to describe the functionality of the catch and trap interface: <i>Alice</i>, <i>Bob</i>, and <i>Chris</i> are routers connected to one another shown in Figure 4. The remote management application <i>Timothy</i> is suspecting that <i>Bob</i> has been compromised. <i>Timothy</i> will send a <i>suspend</i> request to the out-going prevention module of <i>Alice</i> to catch and hold one outgoing LSA (<i>LSA<sub>A</sub></i>, which should be sent to <i>Bob</i>). Now, <i>Timothy</i> will use the Catch and Trap interface on <i>Chris</i>. After the request, <i>Chris</i> knows that he should look at all the OSPF PDUs from <i>Bob</i> and check if one of them is <i>LSA<sub>A</sub></i>. At this point, <i>Timothy</i> will notify <i>Alice</i> to release <i>LSA<sub>A</sub></i>. Now, if <i>Chris</i> catches <i>LSA<sub>A</sub></i>, he will trap/notify <i>Timothy</i> immediately. If, after <math>\delta</math> amount of time, he cannot find <i>LSA<sub>A</sub></i>, he will also notify <i>Timothy</i> with a Catch-failure report. This catch-and-trap MIB interface facility can be used to efficiently handle compromised routers." (36) [SYM_P_0070381]</p> <p>"Detection Notifications: A particular trusted security management application might be interested in knowing if one particular type of report has been updated in the MIB. Traps/Event notifications are very useful in this situation. In JiNao, this security management application can express its interest in certain types of information through the SNNMP MIB interface. The JiNao agent, upon receiving the request, will start to generate traps/events for the application when an event occurs." (33) [SYM_P_0070578]</p>
18	The method of claim 1,	"One approach is to collect data from separate hosts on a network for processing by a centralized intrusion detection system

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

338 Claim number	Claim Term	JiNao Report (printed publication)
	wherein the network packets comprise TCP/IP packets.	<p>[2][3]. The other approach is to target network traffic at the service and protocol levels [6][7]. Our effort is close to the second approach with a few exceptions. First, we are interested in protecting network infrastructure and particularly focus on routing and management capabilities. Therefore, the target of analysis is mainly on specific protocol traffic instead of general data traffic. Second, the proposed protocol analysis approach in our architecture design is unique which analyzes the logical behavior of routing and management protocols in order to identify the set of states that are indicative of security attacks. Third, network management functionalities are part of the integrated system design. Through these functionalities, the intrusion detection system can be incorporated into existing management framework as an extension of fault management." (2) [SYM_P_0070547]</p> <p>The intrusion detection solution prototyped in this project can be applied to any network environment that uses OSPF routing protocol. (12) [SYM_P_0070557]</p> <p>"As we mentioned earlier, the interception and prevention modules together are acting like a firewall to filter out any packet with clear security violation. Putting this firewall right within IP (in the kernel space) allows us to protect a set of applications (e.g., Gated, SNMP, HTTP) without modifying their source codes." (15) [SYM_P_0070560]</p> <p>"In this project, we focus our effort on the protection of the network infrastructure since the attacks on the routers/switches have the potential of disrupting a large scale of information services on which the national defense and economy may depend." (1) [SYM_P_0070546]</p> <p>"A local subsystem is associated with a router/switch to function as a security filter and analyzes the incoming packets from its neighbors." (3) [SYM_P_0070548]</p> <p>"A JiNao local subsystem logically resides in a router or just next to it." (14) [SYM_P_0070559]</p> <p>"The basic statistical approach is to compare a subject's short-term behavior with the subject's historical or long-term behavior. A subject is context-dependent, which can be a user of a computer system, a credit card holder, or one of the neighbor routers in</p>
19	The method of claim 1, wherein the network entity comprises a gateway, a router, or a proxy server.	

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

Claim number	Claim term	JiNao Report (printed publication)
24	A computer program product, disposed on a computer readable medium, the product including instructions for causing a processor to: receive network packets handled by a network entity;	<p>the case of this project. In comparing short-term behavior with long-term behavior, the statistical component is concerned both with long-term behaviors that do not appear in short-term behavior, and with short-term behaviors that are not typical of long-term behavior." (18) [SYM_P_0070563]</p> <p>"This three-year project aims at designing and developing a software system for protecting against intruders from breaking into network routers, switches, and network management channels." (1) [SYM_P_0070546]</p> <p>"In the early stage, intrusion detection system [sic] were designed around the analysis of a single host's audit trail. With the proliferation of computer networks, many of the intrusion detection systems began to extend the techniques to networks of computers. Most of the current network intrusion detection efforts have taken one of the two following approaches. One approach is to collect data from separate hosts on a network for processing by a centralized intrusion detection system [2][3]. The other approach is to target network traffic at the service and protocol levels [6][7]. Our effort is close to the second approach with a few exceptions. First, we are interested in protecting network infrastructure and particularly focus on routing and management capabilities. Therefore, the target of analysis is mainly on specific protocol traffic instead of general data traffic." (2) [SYM_P_0070547]</p> <p>"A local subsystem is associated with a router/switch to function as a security filter and analyze the incoming packets from its neighbors." (3) [SYM_P_0070548]</p> <p>"2.2.1.1 Interception/Redirection Module. The responsibility of the interception module is to <i>redirect</i> the target protocol information flow to the prevention layer for rule checking". (5) [SYM_P_0070550]</p> <p>"TP/IPSEC: The PDUs can be intercepted at the IP layer." (14) [SYM_P_0070559]</p>

## Scalable Intrusion Detection for the Emerging Network “JiNao Report”

Class Claim number	Class Claim Item	JiNao Report (printed publication)
	build at least one long-term and at least one short-term statistical profile from at least one measure of the network packets,	<p>See also Fig. 1 (4); [SYM_P_0070549] Fig. 3, (17) [SYM_P_0070562]</p> <p>“2.2.1.3.1 Statistical Analysis Module Intrusion detection using statistical analysis is founded on the contention that behavioral signatures exist for either users’ usage profiles or protocol execution patterns (in this case, network routing an management protocols) and intrusion will result in abnormal signatures. Any behavior deviating from the normal signature will be considered as an anomaly and appropriate alarms can be triggered. This module provides the capability to detect intrusions that exploit previously unknown vulnerabilities.” (5) [SYM_P_0070550]</p> <p>“4.1.3.1 Statistical Analysis Module In the area of computer security, statistical analysis has been reported in various projects in the literature, for example, the NIDES project at SRI [11] Wisdom and Sense at Los Alamos National Laboratory [12], and Haystack project [13] at Haystack Laboratories. Among these examples, the NIDES project at SRI is most extensive in its scope and development. It also has the most complete documentations available to the general public. With the understanding of statistical analysis’s general applicability, we will adapt NIDES’s statistical algorithm in our approach as a starting point and modify it as necessary.</p> <p>The basic statistical approach is to compare a subject’s short-term behavior with the subject’s historical or long-term behavior.” (18) [SYM_P_0070563]</p> <p>Measures: Aspects of subject behavior are represented as measures (e.g., packet and LSA arrival frequencies in terms of their types or sources). For each measure, we will construct a probability distribution of short-term and long-term behaviors. For example, for the packet types received, the long-term probability distribution would consist of the historical probabilities with which different types of packets have been received, and the short-term probability distribution would consist of the recent probabilities with which different types [sic] packets have been received. In this case, the categories to which probabilities are attached are the names of packet types, which are learned by the system as they are received. We would classified [sic] the JiNao measures into two groups: activity intensity and audit record distribution measures. These two types of measures serve different dimensional purposes. The activity measures determine whether the volume of general activity generated in the recent</p>

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

358 (Claim number)	Claim Item	JiNao Report (printed publication)
		<p>past (depending on the half-life of the measure, here "recent past" corresponds to the time span of last several half-lives) is normal. These measures can detect bursts of activity or prolonged activity that is abnormal, primarily based on the volume of audit data generated. The audit record distribution measure determines whether, for recently observed activity (say, the last few hundred audit records received), the types of actions being generated across neighbors are normal. For example, we might find that the last 200 routing packets received contained 120 of Hello packets, 15 of Database Description packets, 10 of Link State Request packets, 35 of Link State Update packets, and 20 of Acknowledgment [sic] packets. These data are compared to a profile of previous activity (generated over the last few months) to determine whether or not the distribution of activity types generated in the recent past (i.e., the last few hundred audit records) is unusual.</p> <p>...</p> <p>For the long-term profile, the long-term aging factor is applied to the historical data at each update, and then the new information is folded in. For the short term profile, the short-term aging factor is applied to the profile with each audit record and the current audit record is folded in." (19) [SYM_P_0070564]</p>
the measure monitoring data transfers, errors, or network connections;		<p>"A new profile (long-term and short-term) is created whenever a new subject is first encountered." (24) [SYM_P_0070569]</p> <p>"We would classified [sic] the Ji-Nao measures into two groups: activity intensity and audit record distribution measures. These two types of measures serve different dimensional purposes. The activity measures determine whether the volume of general activity generated in the recent past (depending on the half-life of the measure, here "recent past" corresponds to the time span of last several half-lives) is normal. These measures can detect bursts of activity or prolonged activity that is abnormal, primarily based on the volume of audit data generated. The audit record distribution measure determines whether, for recently observed activity (say, the last few hundred audit records received), the types of actions being generated across neighbors are normal. For example, we might find that the last 200 routing packets received contained 120 of Hello packets, 15 of Database Description packets, 10 of Link State Request packets, 35 of Link State Update packets, and 20 of Acknowledgment [sic] packets. These data are compared to a profile of previous activity (generated over the last few months) to determine whether or not the distribution of activity types generated in the recent past (i.e., the last few hundred audit records) is unusual." (19) [SYM_P_0070564]</p>

# Scalable Intrusion Detection for the Emerging Network "JINao Report"

Claim number	Claim term	JINao Report (printed publication)
	compare at least one short-term and at least one long-term statistical profile; and	<p>"One of the important features of the JINao system is that it is adaptive to changing network conditions/configurations. This implies that the set of rules upon which the prevention module operates on or the threshold parameters which the statistical module uses to distinguish normal from abnormal behavior or the set of minimum detecting sequences employed by the protocol analysis module may need to be changed dynamically in response to changing network conditions. For instance, should a new point of network connectivity come up, the normal traffic profiles would need to be modified to account for the traffic from the new connection." (29) [SYM_P_0070574]</p> <p>"The basic statistical approach is to compare a subject's short-term behavior with the subject's historical or long-term behavior. A subject is context-dependent, which can be a user of a computer system, a credit card holder, or one of the neighbor routers in the case of this project. In comparing short-term behavior with long-term behavior, the statistical component is concerned both with long-term behaviors that do not appear in short-term behavior, and with short-term behaviors that are not typical of long-term behavior." (18) [SYM_P_0070563]</p> <p>"The Q Statistic: The degree of difference between a long-term and short-term profile for a measure is quantified using a chi-square-like statistic, comparing observation (the short-term profile) to expectation (the long-term profile)." (20) [SYM_P_0070565]</p> <p>"The range of the Q values is expressed in terms of the degree of similarity between the short-term profile and the long-term profile with larger numbers representing less similarity." (23) [SYM_P_0070568]</p> <p>"For each audit record generated by a subject, the statistical module generates a single test statistic value, denoted <math>T^2</math>, that summarizes the degree of abnormality in the subject's behavior in the near past." p. 19. [SYM_P_0070564]</p> <p>"The degree of difference between a long-term profile and short-term profile for a measure is quantified using a chi-square-like statistic, comparing observation (the short-term profile) to expectation (the long-term profile). The resultant numerical value is call</p>

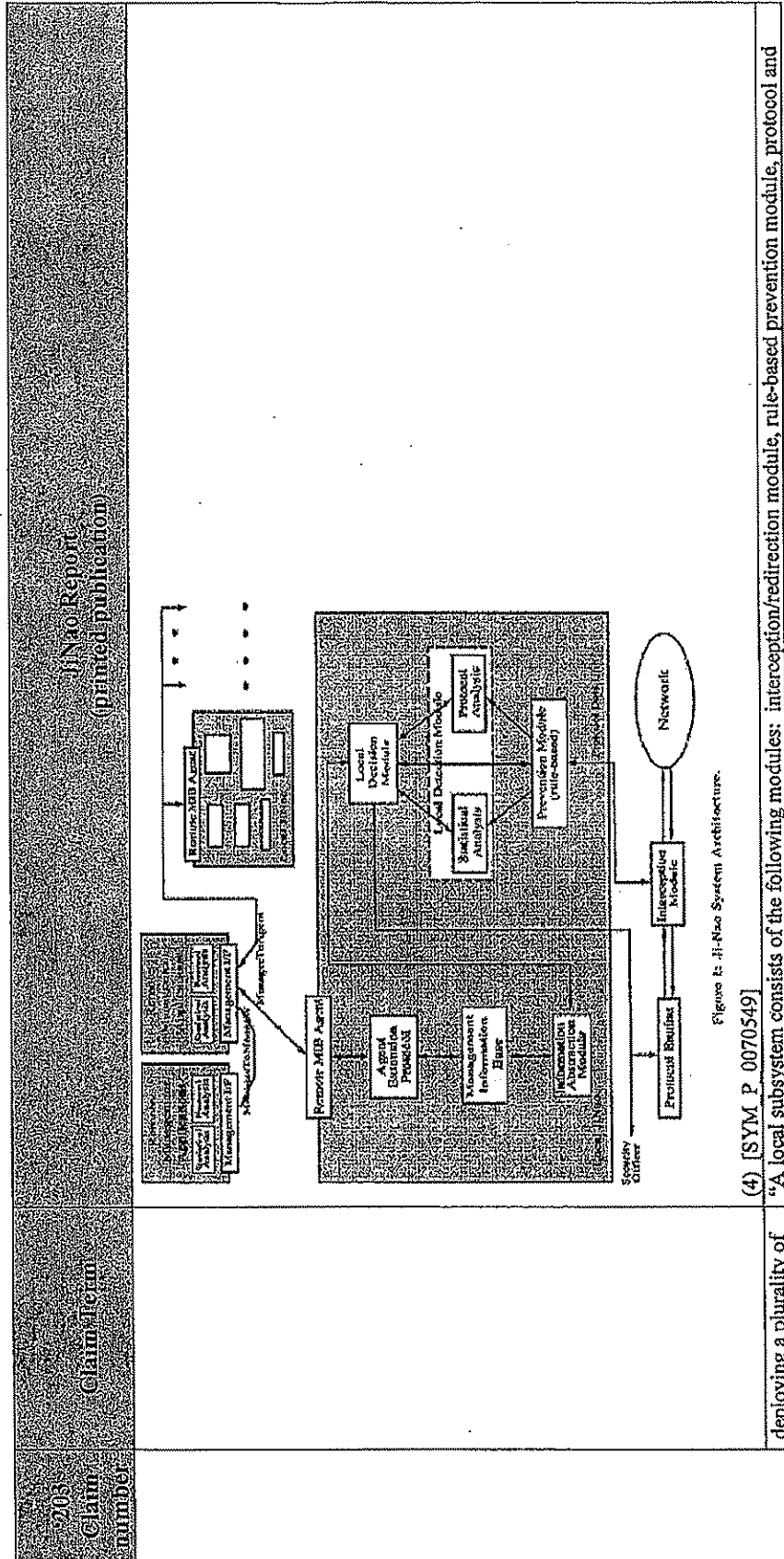
# Scalable Intrusion Detection for the Emerging Network “JiNao Report”

Claim number	Claim Term	JiNao Report (printed publication)
	determine whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.	<p><i>Q</i> in NIDES,” (20) [SYM P 0070563]            Whenever short-term behavior is sufficiently unlike long-term behavior, a warning flag is raised. (18) [SYM P 0070563]            “The statistical component issues a warning only if the current short-term behavior is very unlike long-term behavior relative to the amount of deviation between these types of behaviors that it has seen in the past.” (18) [SYM P 0070563]</p>

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

Claim number	Claim term	JiNao Report (printed publication)
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	<p>"This three-year project aims at designing and developing a software system for protecting against intruders from braking into network routers, switches, and network management channels. ... In this project, we focus our effort on the protection of the network infrastructure since the attacks on the routers/switches have the potential of disrupting a large scale of information services on which the national defense and economy may depend. ... In particular, we will conduct logical and statistical analysis of network routing and management protocols to construct a scalable distributed intrusion detection system for the emerging internetwork environment." (1) [SYM_P_0070546]</p> <p><b>"2.1 Architecture Overview</b></p> <p>Figure 1 illustrates the architecture design of our intrusion detection system. At the top level, there are two subsystems: namely, local detection subsystem and remote management subsystem. ...</p> <p>A local subsystem is associated with a router/switch to function as a security filter and analyze the incoming packets from its neighbors....</p> <p>A remote management subsystem can oversee several routers/switches. Some intrusions, like doorknob rattling attack, which may be difficult to detect at the local level can be made easier by checking the global status across several routers/switches. While it is not within the scope of this project, we expect that the detection/analysis functions implemented in the local subsystem can be extended to a global level and correlate intrusion events among several routers. The management capability, which is based on SNMP framework, can logically be further extended among management nodes in a hierarchical fashion to establish a status map for an autonomous system." (3) [SYM_P_0070548]</p> <p>See Figure 1: Ji-Nao System Architecture [showing multiple Ji-Nao systems] (4) [SYM_P_0070549]</p>

# Scalable Intrusion Detection for the Emerging Network "JiNao Report"



## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

270 Claim number	Claim term network monitors in the enterprise network;	JiNao Report (printed publication)
		<p>statistical-based detection modules, decision module, and information abstraction module. It also includes a management information base (MIB) and a remote MIB agent functions which provide access to remote management applications." (3) [SYM_P_0070548]</p> <p>See Figure 1: Ji-Nao System Architecture [showing multiple Ji-Nao systems] (4) [SYM_P_0070549]</p> <p>"2.2.1.3 Detection Module If a packet passes through the prevention module, it will be forwarded to the protocol engine for execution and to the local detection module which performs statistical- and protocol-based intrusion checks. ... The decision information can be either derived from the input of detection modules or come from the global detection module and the remote management applications through the MIB interface. Therefore, our design will allow for a certain degree of automated responses through the adoption of network management framework." (5) [SYM_P_0070550]</p> <p>"2.2.1.4 Local Decision Module The decision module on one hand serves as a coordinator to correlate the information from the prevention and the detection modules for determining if any intrusion has occurred and what actions need to be taken. ... Through both local and remote MIB agents, the decision module provides its local view of neighbor status to remote management applications for identifying any global scale of attacks. It also relays commands from remote management applications to the local prevention module and detection modules." (6) [SYM_P_0070551]</p> <p>"2.2.2 Remote Subsystem In the current scope of the project, a remote subsystem consists of a set of management applications for monitoring and controlling a few local detection subsystems. It is expected that a management application would be able to re-configure the local detection system dynamically. With this configurability, the local detection subsystem can respond to intrusion differently under different situations. Ideally, as a natural extension of the current scope of the project, we expect that a remote subsystem can also implement similar detection capabilities in order to detect a larger scale of orchestrated attack. We realize that some attacks (for instance, door-knob rattling attack) can only be detected on a more global scale. One approach in dealing with these attacks is for the management applications to communicate with their local detection agents in order to form a global view of the domain surrounding this remote subsystem. The notion of global detection can be further extended to cover more than one remote subsystem, either in a distributed or</p>

# Scalable Intrusion Detection for the Emerging Network "JiNao Report"

Claim number	Claim Term	JiNao Report (printed publication)
		hierarchical fashion. ... Two or more remote subsystems can establish a global view of the network by exchanging detection information from their domains. If the remote subsystems are organized in a distributed fashion, the communication among them is through manager to manager operation. Otherwise, the communication will be manager to agent operation when the system is in a hierarchical architecture." (6-7) [SYM_P_0070551- SYM_P_0070552]
		"Finally, the deployment of the intrusion detection system does not require installation of Ji-Nao modules to each every routing entity in the network in order to operate, although wider deployment generally affords better overall detection capability." (12) [SYM_P_0070557]
	detecting, by the network monitors, suspicious network activity	"2.2.1.3 Detection Module If a packet passes through the prevention module, it will be forwarded to the protocol engine for execution and to the local detection module which performs statistical- and protocol-based intrusion checks. ... The decision information can be either derived from the input of detection modules or come from the global detection module and the remote management applications through the MIB interface. Therefore, our design will allow for a certain degree of automated responses through the adoption of network management framework." (5) [SYM_P_0070550]
		"2.2.1.4 Local Decision Module The decision module on one hand serves as a coordinator to correlate the information from the prevention and the detection modules for determining if any intrusion has occurred and what actions need to be taken. ... Through both local and remote MIB agents, the decision module provides its local view of neighbor status to remote management applications for identifying any global scale of attacks. It also relays commands from remote management applications to the local prevention module and detection modules." (6) [SYM_P_0070551]
		"Whenever short-term behavior is sufficiently unlike long-term behavior, a warning flag is raised." (18) [SYM_P_0070563]
		"The statistical component issues a warning only if the current short-term behavior is very unlike long-term behavior relative to the amount of deviation between these types of behaviors that it has seen in the past." (18) [SYM_P_0070563]

## Scalable Intrusion Detection for the Emerging Network “JiNao Report”

203 Alarm number	Alarm term	JiNao Report (printed publication)
based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};		<p>“We would classified [sic] the Ji-Nao measures into two groups: activity intensity and audit record distribution measures. These two types of measures serve different dimensional purposes. The activity measures determine whether the volume of general activity generated in the recent past (depending on the half-life of the measure, here “recent past” corresponds to the time span of last several half-lives) is normal. These measures can detect bursts of activity or prolonged activity that is abnormal, primarily based on the volume of audit data generated. The audit record distribution measure determines whether, for recently observed activity (say, the last few hundred audit records received), the types of actions being generated across neighbors are normal. For example, we might find that the last 200 routing packets received contained 120 of Hello packets, 15 of Database Description packets, 10 of Link State Request packets, 35 of Link State Update packets, and 20 of Acknowledgment [sic] packets. These data are compared to a profile of previous activity (generated over the last few months) to determine whether or not the distribution of activity types generated in the recent past (i.e., the last few hundred audit records) is unusual.” (19) [SYM_P_0070564]</p> <p>“One of the important features of the JiNao system is that it is adaptive to changing network conditions/configurations. This implies that the set of rules upon which the prevention module operates on or the threshold parameters which the statistical module uses to distinguish normal from abnormal behavior or the set of minimum detecting sequences employed by the protocol analysis module may need to be changed dynamically in response to changing network conditions. For instance, should a new point of network connectivity come up, the normal traffic profiles would need to be modified to account for the traffic from the new connection.” (29) [SYM_P_0070574]</p>
generating, by the monitors, reports of said suspicious activity; and		<p>“Functionally, the local decision module interfaces with both the detection modules and the local MIB agent software. It receives input from the detection modules regarding local intrusion activity as inferred by observing the neighbor’s behavior. It also interacts with the local MIB agent to gather intrusion detection information obtained from remote JiNao agents and uses it in conjunction with the data reported from the detection modules to make decisions on intrusions. Finally, it also interacts with the protocol engine to take appropriate steps when an intrusion is detected.” (29) [SYM_P_0070574]</p> <p>“4.1.5. Information Abstraction Module (IAM) 4.1.5.1 IAM Functions The IAM serves as an interface module between the JiNao local intrusion detection subsystem and the remote</p>

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

Claim number	Claim term	JiNaoReport (printed publication)
		<p>JiNao modules as well as other network management applications. In propagating local intrusion detection results to the outside, the IAM aggregates local detection results and converts them into the MIB format." (31) [SYM_P_0070576]</p> <p>"Local Detection Results: The local decision module, after performing analysis on the events or messages, makes decisions about whether certain intrusion attacks have happened. ... Each piece of information should be represented as a JiNao report table entry (<i>i.e.</i>, JiNaoReportTableEntry)." (33) [SYM_P_0070578]</p>
	<p>automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.</p>	<p>"The management capability, which is based on SNMP framework, can logically be further extended among management nodes in a hierarchical fashion to establish a status map for an autonomous system." (3) [SYM_P_0070548]</p> <p>"Two or more remote subsystems can establish a global view of the network by exchanging detection information from their domains. If the remote subsystems are organized in a distributed fashion, the communication among them is through manager to manager operation. Otherwise, the communication will be manager to agent operation when the system is in a hierarchical architecture." (7) [SYM_P_0070552]</p> <p><b>"3.2 Scalability</b> Even though the current scope of the project focuses on the development of local detection capabilities, we expect the system design can be easily extended to a regional and even a more global level. While it is not within the scope of this project, we expect the detection/analysis functions implemented in the local subsystem can be extended to a global level and correlate intrusion events among several routers. The extension to a global level can be hierarchical where several regional management stations can aggregate their detection information to a higher level for establishing a global view of the routing domain status. The communication of this extension can be provided through SNMP ManagerToManager operations. (13) [SYM_P_0070558]</p> <p>"While it is more efficient to detect intrusions locally, as far as possible, there are cases where only a global agent can make a determination of whether an intrusion has taken place based on information gathered from several local JiNao decision modules." (29) [SYM_P_0070574]</p>

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

205 @lam number	@lam:tem	JiNaoReport (printed publication)
		<p>"The fact that the local decision module uses information disseminated by the remote JiNao agents in order to make a decision on intrusion leads to a scalable architecture. Indeed, in the converse situation, if the local agents had to forward all their detection information to the global agent in order for the global agent to make the decision, the global agent would become the centralized decision maker and the architecture would not scale. In our system global information is utilized locally to make a globally aware local decision regarding intrusion. Moreover, the architecture also provides for monitoring attacks which can only be detected at a higher network level." (31) [SYM_P_0070576]</p> <p>"Scope of impact information is used by a set of distributed JiNao decision modules in order to better enhance the accuracy of intrusion detection decisions. For example, ... a higher-level decision module, i.e. one that has access to observations on a larger topological region, can correlate multiple detections from low-levels according to their respective scope of impact, and to reach a more accurate detection decision." (32) [SYM_P_0070577]</p> <p>"The following example is used to describe the functionality of the catch and trap interface: <i>Alice</i>, <i>Bob</i>, and <i>Chris</i> are routers connected to one another shown in Figure 4. The remote management application <i>Timothy</i> is suspecting that <i>Bob</i> has been compromised. <i>Timothy</i> will send a <i>suspend</i> request to the out-going prevention module of <i>Alice</i> to catch and hold one outgoing LSA (<i>LSA<sub>A</sub></i>, which should be sent to <i>Bob</i>). Now, <i>Timothy</i> will use the Catch and Trap interface on <i>Chris</i>. After the request, <i>Chris</i> knows that he should look at all the OSPF PDUs from <i>Bob</i> and check if one of them is <i>LSA<sub>A</sub></i>. At this point, <i>Timothy</i> will notify <i>Alice</i> to release <i>LSA<sub>A</sub></i>. Now, if <i>Chris</i> catches <i>LSA<sub>A</sub></i>, he will trap/notify <i>Timothy</i> immediately. If, after <math>\delta</math> amount of time, he cannot find <i>LSA<sub>A</sub></i>, he will also notify <i>Timothy</i> with a Catch-failure report. This catch-and-trap MIB interface facility can be used to efficiently handle compromised routers." (36) [SYM_P_0070581]</p> <p>"<b>Detection Notifications:</b> A particular trusted security management application might be interested in knowing if one particular type of report has been updated in the MIB. Traps/Event notifications are very useful in this situation. In JiNao, this security management application can express its interest in certain types of information through the SNMP MIB interface. The JiNao agent, upon receiving the request, will start to generate traps/events for the application when an event occurs." (33) [SYM_P_0070578]</p>

## Scalable Intrusion Detection for the Emerging Network “JiNao Report”

Claim number	Claim term	JiNao Report (printed publication)
2	The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.	<p><b>“3.2 Scalability</b></p> <p>Even though the current scope of the project focuses on the development of local detection capabilities, we expect the system design can be easily extended to a regional and even a more global level. While it is not within the scope of this project, we expect the detection/analysis functions implemented in the local subsystem can be extended to a global level and correlate intrusion events among several routers. The extension to a global level can be hierarchical where several regional management stations can aggregate their detection information to a higher level for establishing a global view of the routing domain status. The communication of this extension can be provided through SNNMP ManagerToManager operations. (13) [SYM_P_0070558]</p> <p>“While it is more efficient to detect intrusions locally, as far as possible, there are cases where only a global agent can make a determination of whether an intrusion has taken place based on information gathered from several local JiNao decision modules.” (29) [SYM_P_0070574]</p> <p>“The fact that the local decision module uses information disseminated by the remote JiNao agents in order to make a decision on intrusion leads to a scalable architecture. Indeed, in the converse situation, if the local agents had to forward all their detection information to the global agent in order for the global agent to make the decision, the global agent would become the centralized decision maker and the architecture would not scale. In our system global information is utilized locally to make a globally aware local decision regarding intrusion. Moreover, the architecture also provides for monitoring attacks which can only be detected at a higher network level.” (31) [SYM_P_0070576]</p> <p>“Scope of impact information is used by a set of distributed JiNao decision modules in order to better enhance the accuracy of intrusion detection decisions. For example, ... a higher-level decision module, i.e. one that has access to observations on a larger topological region, can correlate multiple detections from low-levels according to their respective scope of impact, and to reach a more accurate detection decision.” (32) [SYM_P_0070577]</p> <p>“The following example is used to describe the functionality of the catch and trap interface: <i>Alice</i>, <i>Bob</i>, and <i>Chris</i> are routers connected to one another shown in Figure 4. The remote management application <i>Timothy</i> is suspecting that <i>Bob</i> has been compromised. <i>Timothy</i> will send a <i>suspend</i> request to the out-going prevention module of <i>Alice</i> to catch and hold one outgoing LSA (<i>LSA<sub>x</sub></i>, which should be</p>

## Scalable Intrusion Detection for the Emerging Network “JiNao Report”

205 Claim number	Claim Term	JiNao Report (printed publication)
		<p>sent to Bob). Now, Timothy will use the Catch and Trap interface on Chris. After the request, Chris knows that he should look at all the OSPF PDUs from Bob and check if one of them is LS4. At this point, Timothy will notify Alice to release LS4. Now, if Chris catches LS4, he will trap/notify Timothy immediately. If, after <math>\delta</math> amount of time, he cannot find LS4, he will also notify Timothy with a Catch-failure report. This catch-and-trap MIB interface facility can be used to efficiently handle compromised routers.” (36) [SYM_P_0070581]</p> <p>“<b>Detection Notifications:</b> A particular trusted security management application might be interested in knowing if one particular type of report has been updated in the MIB. Traps/Event notifications are very useful in this situation. In JiNao, this security management application can express its interest in certain types of information through the SNMP MIB interface. The JiNao agent, upon receiving the request, will start to generate traps/events for the application when an event occurs.” (33) [SYM_P_0070578]</p>
3	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	<p>“Therefore, our design will allow for a certain degree of automated responses through the adoption of network management framework.” (5) [SYM_P_0070550]</p> <p>“One of the important features of the JiNao system is that it is adaptive to changing network conditions/configurations. This implies that the set of rules upon which the prevention module operates on or the threshold parameter which the statistical module uses to distinguish normal from abnormal behavior or the set of minimum detecting sequences employed by the protocol analysis module may need to be changed dynamically in response to changing network conditions.” (29) [SYM_P_0070574]</p> <p>“[B]ased on the decision it arrives at, the LDecM could initiate these changes itself. For instance, if it detected suspicious activity, it could activate additional rules in the prevention module or adjust thresholds in the statistical module. ... The LDecM interacts with the protocol engine in order to take appropriate action if an intrusion is suspected/detected. For instance, when suspicious activity is detected it may instruct the protocol engine to turn on certain special modes of operation e.g. detailed logging of messages and protocol events, log information relating to route updates and modifications etc.. The LDecM can also take appropriate defensive measures. This can include turning an interface off when a router connected via that interface has been detected to be faulty/compromised, issuing commands to undo the effects of recent route update messages, if any,</p>

## Scalable Intrusion Detection for the Emerging Network “JiNao Report”

203 Claim number	Claim Item	JiNao Report (printed publication)
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	<p>from the compromised router, etc.” (30) [SYM_P_0070575]</p> <p><b>“3.3 Interoperability</b> We expect that an intrusion detection system will be part of the network management framework in order to best capitalize its benefits. SNMP is a network management information exchange protocol that has been implemented and widely deployed in the existing networks. Since SNMP is the industrial <i>de facto</i> standard, our system will be able to integrated [sic] with other SNMP –based system or security applications with relative ease. Another aspect of the interoperability (including module reusability) is related to the questions of</p> <ol style="list-style-type: none"> <li>1. identifying well-understood building blocks/modules for the intrusion detection systems,</li> <li>2. clearly defining the functionality and interfaces for these modules, and</li> <li>3. defining the basic protocol for inter-operation among the appropriate modules.</li> </ol> <p>Currently, there is a joint effort to address the system interoperability and module reusability issues among DARPA/TTO sponsored projects, especially among the intrusion detection community, in order to fully take advantage of the investment and bring forth a better synergistic effect. Our architectural design is consistent with the objectives of this joint effort. We strive to clearly define the common modules (interception, detection/analysis, decision, and management and agent) by specifying their functions and interfaces. As a member of the CIDF (Common Intrusion Detection Framework) working group, we expect that, as the CIDF joint effort progress further, necessary modifications can be made to further enhance the interoperability and reusability of our system with other systems.” (13-14) [SYM_P_0070558- SYM_P_0070559]</p> <p><b>“4.1.5 Information Abstraction Module (IAM)</b> <b>4.1.5.1 IAM Functions</b> The IAM serves as an interface module between the JiNao local intrusion detection subsystem and the remote JiNao modules as well as other network management applications. In propagating local intrusion detection results to the outside, the IAM aggregates local detection results and converts them into the MIB format. In updating the local detection and prevention modules with new rule sets, the IAM receives and processes requests from the remote subsystems through the JiNao MIB interface.” (31) [SYM_P_0070576]</p>

## Scalable Intrusion Detection for the Emerging Network “JiNao Report”

205 Claim number	Claim Term	JiNao Report (printed publication)
5	The method of claim 1, wherein the enterprise network is a TCP/IP network.	<p>See also 4.1.6 Management Information Base</p> <p><b>“Target Environment:</b> The intrusion detection solution prototyped in this project can be applied to any network environment that uses OSPF routing protocol. Examples of such environments are networks consisting of only OSPF-based IP routers, networks containing autonomous systems that are using OSPF protocol, and networks including ATM and IP-Switching technologies but uses OSPF at the IP level.” (12) [SYM_P_0070557]</p> <p>“Depending on the target protocols under JiNao’s protection, interception module can be placed in multiple protocol layers (Figure 2): IP/IPSEC: The PDUs can be intercepted at the IP layer. In many operating systems (e.g., Linux and BSD), the kernel-level IP packet interception has been supported. For example, the <i>ipfwadm</i> package is for flexible implementation of firewall mechanisms in the kernel. If certain IPSEC options are turned on, we should redirect the PDUs after the security checks performed by the IPSEC layer. This will eliminate immediately PDUs violating the protection provided by IPSEC.</p> <p><b>Device Driver:</b> Network hardware device driver (e.g., EtherNet device driver) is usually not a good place for interception because IP packets can be fragmented (large PDUs), encapsulated (tunneled PDUs), and authenticated/encrypted (IPSECed PDUs). Performing interception at this level may introduce unnecessary system complexity and should be avoided unless the redirection function is unavailable in all other layers.</p> <p><b>Higher-Layer Protocols:</b> Sometimes, it is necessary to perform interception in layers beyond IP. For example, in protecting SNMP, (especially SNMPv2 and v3), the SNMP PDU might be encrypted. Under this case, we should intercept the PDU flow after the authentication and decryption process.” (14) [SYM_P_0070559]</p> <p>“In this project, we focus our effort on the protection of the network infrastructure since the attacks on the routers/switches have the potential of disrupting a large scale of information services on which the national defense and economy may depend.” (1) [SYM_P_0070546]</p> <p>“A local subsystem is associated with a router/switch to function as a security filter and analyze the incoming packets from its neighbors.” (3) [SYM_P_0070548]</p>
6	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers,	

## Scalable Intrusion Detection for the Emerging Network "JiNao Report"

Claim number	Claim term	JiNao Report (printed publication)
	proxy servers}.	<p>"A JiNao local subsystem logically resides in a router or just next to it." (14) [SYM_P_0070559]</p> <p>"The basic statistical approach is to compare a subject's short-term behavior with the subject's historical or long-term behavior. A subject is context-dependent, which can be a user of a computer system, a credit card holder, or one of the neighbor routers in the case of this project. In comparing short-term behavior with long-term behavior, the statistical component is concerned both with long-term behaviors that do not appear in short-term behavior, and with short-term behaviors that are not typical of long-term behavior." (18) [SYM_P_0070563]</p>
7	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	<p>"The management capability, which is based on SNMP framework, can logically be further extended among management nodes in a hierarchical fashion to establish a status map for an autonomous system." (3) [SYM_P_0070548]</p> <p><b>"2.2.2 Remote Subsystem</b></p> <p>In the current scope of the project, a remote subsystem consists of a set of management applications for monitoring and controlling a few local detection subsystems. It is expected that a management application would be able to re-configure the local detection system dynamically. With this configurability, the local detection subsystem can respond to intrusion differently under different situations. Ideally, as a natural extension of the current scope of the project, we expect that a remote subsystem can also implement similar detection capabilities in order to detect a larger scale of orchestrated attack. We realize that some attacks (for instance, door-knob rattling attack) can only be detected on a more global scale. One approach in dealing with these attacks is for the management applications to communicate with their local detection agents in order to form a global view of the domain surrounding this remote subsystem. The notion of global detection can be further extended to cover more than one remote subsystem, either in a distributed or hierarchical fashion.</p> <p>...</p> <p>Two or more remote subsystems can establish a global view of the network by exchanging detection information from their domains. If the remote subsystems are organized in a distributed fashion, the communication among them is through manager to manager operation. Otherwise, the communication will be manager to agent operation when the system is in a hierarchical architecture." (6-7) [SYM_P_0070551- SYM_P_0070552]</p>